UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/764,602 | 01/18/2001 | Jun Hirai | SONYJP 3.0-138 | 6651 |

530 7590 03/17/2008

LERNER, DAVID, LITTENBERG,
KRUMHOLZ & MENTLIK
600 SOUTH AVENUE WEST
WESTFIELD, NJ 07090

| EXAMINER | |
|---|---|
| COLIN, CARL G | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2136 | |

| MAIL DATE | DELIVERY MODE |
|---|---|
| 03/17/2008 | PAPER |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 09/764,602 | HIRAI, JUN | |
| | Examiner | Art Unit | |
| | CARL COLIN | 2136 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *11,14-16,18,20 and 53-62* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *11,14-16,18,20 and 53-62* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

## DETAILED ACTION

### *Response to Arguments*

1. In response to communications filed on 11/23/2007, the following claims 11, 14-16, 18, 20, and 53-62 are presented for examination.

1.1 Applicant's remarks, pages 2-4, filed on 11/23/2007, with respect to the rejection of claims 11, 14-16, 18, 20, and 53-6 have been fully considered, but they are not fully persuasive. Regarding claim 11, Applicant argues that Levy and Morito does not disclose monitoring to determine whether a particular piece of content is distributed with authorization of the owner. However, this limitation is disclosed in Stefik as found in claim 14. Therefore, upon further consideration a new ground of rejection is made in view of Stefik and the rejection is set forth below.

### *Claim Rejections - 35 USC § 103*

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

**Claims 11, 14-16, 18, 20, and 53-62** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 6,505,160 to **Levy et al** in view of US Patent 6,310,956 to **Morito et al** in view of US Patent 5,715,403 to **Stefik** *(Applicant's Disclosure).*

**As per claim 11**, **Levy et al.** discloses a distribution method for distributing one or more pieces of content owned by one or more owners from a distributor to one or more receivers and for determining whether the one or more pieces of content have been distributed with authorization of the one or more owners, comprising: **Levy et al.** discloses server1 issuing authentication information (identifier and context information) to servers maintained by the distributors for providing data to the consumer, the servers maintained by the distributors as well as the distributors themselves are interpreted by the Examiner as "distributor" (see column 5, lines 41-50) that meets the recitation of *issuing to the distributor* (server) *authentication information* (identifier, context information and/or metadata) *including time identification information indicating time of issuance*. The identifier of Levy et al meets the recitation of distributor identification assigned to the distributor (see column 8, lines 60-67 and column 3, lines 28-33; and col. 3, line 65- col. 4, line 10); the context information and /or metadata of Levy et al meets the recitation of *(time identification information indicating a time of issuance)* (see column 3, lines 37-45 and column 13, line 15-22).

**Levy et al** further discloses storing a database record of the association between the identifier and the object and any other information used in decoding the object such as its distributor or broadcaster (see column 4, lines 1-8) that meets the recitation of *storing a distribution history for each of the one or more pieces of the content distributed via the*

*predetermined distribution path in association with specific content identification information* (see also column 5, lines 23-36 and column 6, lines 2-28); and

**Levy et al** does not explicitly disclose *monitoring the distribution of one or more pieces of the content in the predetermined distribution path to determine whether the one or more pieces of content distributed by the content distribution operation have been distributed with authorization of the owner of the one or more pieces of content based* time identification information. **Stefik** in an analogous art teaches a system for controlling use and distribution of digital work (content) containing usage right (authentication information) embodied in the digital work (see column 4, lines 35-36), the usage right includes time specification or time stamp (see column 4, lines 25-36 and column 14, lines 49-53). **Stefik** discloses a method for preventing unauthorized distribution of the work (see column 3, lines 8-16) allowing an owner of a digital work to attach usage rights to their work (see column 4, lines 9-11). **Stefik** discloses *monitoring the distribution of one or more pieces of the content in the predetermined distribution path to determine whether the one or more pieces of content distributed by the content distribution operation have been distributed with authorization of the owner of the one or more pieces of content* (column 7, lines 37-44) and further discloses the determination may be based on time as the rights may be dependent on time (see column 31, lines 2-6 and 21-48 and column 54, lines 63-67). (See also time specification for details on time identification information, column 12, line 49 through column 22, line 36). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the distribution system **Levy et al** to provide said monitoring step. One skilled in the art would have been lead to make such a

modification to provide flexibility on how the owner of a digital work may allow it to be distributed as suggested by **Stefik** (see column 3, lines 8-11 and 17-18).

**Levy et al** further discloses the server may *determine a distribution status of the distributed one or more pieces of content based on the distribution history* stored in the database (see column 4, lines 54-61 and column 5, lines 13-16) or (column 4, lines 40 through column 5, line 16 for a better understanding).

**Levy et al** does not explicitly disclose distributing one or more pieces of content via a predetermined distribution path with the time identification information attached thereto. **Morito et al** in an analogous art teaches a copy protection system for protecting content which includes embedding transmission time information into a digital data stream by digital watermarking and comparing the transmission time or broadcast time with the current time at the receiving device to determine if the recording is an attempted unauthorized recording (see abstract and column 7, lines 1-35). (See also column 1, line 49 through column 2, line 8). **Morito et al** also suggests combining the time with the watermark and copy control information (see column 7, line 55 through column 8, line 6 and column 9, lines 20-38). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the features of **Levy et al** using authentication information distributed with the content with the features disclosed by **Morito et al** using broadcast time embedded in the watermark because it would ensure that the broadcast time information is not user set so that a user is unable to circumvent the broadcast time information. One of ordinary skill in the art would have recognized the advantages of using broadcast time embedded in the watermark as part of authentication information for authenticating the content because in the event that the time

difference is not within an acceptable threshold of time the receiver would not be able to further process the content as suggested by **Morito et al** (see column 7, lines 26-35 and column 9, lines 14-20).h

**As per claim 15**, **Levy et al** discloses the limitation of wherein said distribution step embeds the authentication information into one or more pieces of the content using a digital watermarking technique, (see column 8, lines 65-67). (For details see column 8, lines 20-30 and column 8 line 46-col. 9, line 11).

**As per claim 16, Levy et al** discloses the limitation of wherein said distribution step embeds the authentication information into a distribution signal of one or more pieces of the content using a digital watermarking technique, (see column 8, lines 65-67). (For details see column 8, lines 20-30 and column 8 line 46-col. 9, line 11).

**As per claim 18, Levy et al.** discloses the limitation of *extracting only the distribution history associated with specific content by masking the distribution history with a predetermined filter*, for example (see column 13, lines 15-22 and column 10, lines 24-67). **Levy et al** also discloses ISRC, which implicitly or inherently contains predetermined filter and unique identifier (col. 3, lines 24-28).

**As per claim 20**, **Levy et al.** discloses the limitation of *wherein authentication information includes identification information by which said distribution history can be addressed* for example (see column 2, line 61 through col. 3, line 23).

**As per claim 56**, the references as combined above disclose the limitation of wherein the *time identification information indicates a broadcast time and the one or more pieces of content is distributed in a program at the broadcast time* (See Morito et al, column 7, lines 14-35 and column 9, lines 20-38).

**As per claim 57**, the references as combined above disclose the limitation of wherein the *time identification information indicates a broadcast time and the one or more pieces of content is distributed at the broadcast time* (See Morito et al, column 7, lines 14-35 and column 9, lines 20-38).

**As per claim 53**, **Levy et al.** substantially discloses a content distribution system for distributing one or more pieces of content owned by one or more owners to one or more receivers and for determining whether the one or more pieces of content have been distributed with authorization of the one or more owners, comprising: server 1 or server 2 (see fig. 1) (*distribution apparatus) operable to distribute the one or more pieces of content to the one or more receivers* (see column 4, lines 26-32), in other embodiment a distributor, broadcaster, or radio station meets the recitation of distribution apparatus (see col. 10, lines 50-56); **Levy et al** discloses either one of the servers may issue identifier and context information to the other server

and either one may return data or programs to the other server or to the communication application *(receiver)* (see column 5, lines 22-28 and lines 41-50), therefore, server 1 and server 2 meet the recitation of distribution and/or monitoring apparatus; Note that **Levy et al** also discloses different scenarios and embodiments such as transferring streaming or broadcasting one or more pieces of content using various parties such as license server, distributor, broadcasting station and other linking servers in which these parties meet the recitation of distributing and/or monitoring apparatus (see column 4, lines 26-32). **Levy et al** discloses *a monitoring apparatus* (such as server) *operable to issue* as *authentication information of the content* (identifier, context information and/or metadata) (col. 5, lines 26-32) *a set of (a) time identification indicating a time of issuing the authentication information* (see column 3, lines 37-45 and column 13, line 15-22), *and (b) distributor identification information assigned to said distribution apparatus* (distributor or broadcaster ID) (see column 8, lines 60-67 and column 3, lines 30-33). As interpreted by the Examiner, the identifier of Levy et al meets the recitation of distributor identification assigned to the distributor (see column 8, lines 60-67 and column 3, lines 28-33; and col. 3, line 65- col 4, line 10); the context information indicating time of distribution or time of capture and /or metadata (timestamp) of Levy et al meets the recitation of *(time identification indicating a time of issuing the authentication information)* (see column 3, lines 37-45 and column 13, line 15-22). **Levy et al** further discloses the servers are operable to link identifiers to actions, the linking process is a way to monitor playing and distribution of copies of music (see column 13, lines 50-67 and column 3, lines 8-10) that meets the recitation of *a monitoring apparatus operable to monitor a content distribution operation carried out by said distribution apparatus,*

**Levy et al** discloses identifier as well as broadcaster ID (*authentication information)* are embedded with the object forming a linked object during the distribution of one or more pieces of content via a predetermined path to the user's player, tuner, or capture device (see column 4, lines 14-33 and column 10, lines 50-67), that meets the recitation of *said distribution apparatus being operable to conduct the content distribution operation to distribute the of one or more pieces of content via a predetermined distribution path to the one or more receivers,* and further discloses the server stores a database record of the association between the identifier and the object and any other information used in decoding the object such as its distributor or broadcaster (see column 4, lines 1-8) that meets the recitation of *said distribution apparatus being operable to store a distribution history including the authentication information corresponding to the one or more pieces of content distributed via the predetermined distribution path* (see also column 5, lines 23-36 and column 6, lines 2-28);

**Levy et al** does not explicitly disclose *said monitoring apparatus is further operable to determine whether the one or more pieces of content distributed by the content distribution operation have been distributed with authorization of the owner of the one or more pieces of content based on time identification information attached to*. **Stefik** in an analogous art teaches a system for controlling use and distribution of digital work (content) containing usage right (authentication information) embodied in the digital work (see column 4, lines 35-36), the usage right includes time specification or time stamp (see column 4, lines 25-36 and column 14, lines 49-53). **Stefik** discloses a method for preventing unauthorized distribution of the work (see column 3, lines 8-16) allowing an owner of a digital work to attach usage rights to their work (see column 4, lines 9-11). **Stefik** discloses *monitoring the distribution of one or more pieces of*

*the content in the predetermined distribution path to determine whether the one or more pieces of content distributed by the content distribution operation have been distributed with authorization of the owner of the one or more pieces of content* (column 7, lines 37-44) and further discloses the determination may be based on time as the rights may be dependent on time (see column 31, lines 2-6 and 21-48 and column 54, lines 63-67). (See also time specification for details on time identification information, column 12, line 49 through column 22, line 36). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the distribution system **Levy et al** to provide said monitoring step. One skilled in the art would have been lead to make such a modification to provide flexibility on how the owner of a digital work may allow it to be distributed as suggested by **Stefik** (see column 3, lines 8-11 and 17-18).

**Levy et al** further discloses the server may *determine a distribution status of the distributed one or more pieces of content based on the distribution history* stored in the database (see column 4, lines 54-61 and column 5, lines 13-16) or (column 4, lines 40 through column 5, line 16 for a better understanding).

**Levy et al** does not explicitly disclose distributing one or more pieces of content via a predetermined distribution path with the time identification information attached thereto. **Morito et al** in an analogous art teaches a copy protection system for protecting content which includes embedding transmission time information into a digital data stream by digital watermarking and comparing the transmission time or broadcast time with the current time at the receiving device to determine if the recording is an attempted unauthorized recording (see abstract and column 7, lines 1-35). (See also column 1, line 49 through column 2, line 8).

**Morito et al** also suggests combining the time with the watermark and copy control information (see column 7, line 55 through column 8, line 6 and column 9, lines 20-38). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the features of **Levy et al** using authentication information distributed with the content with the features disclosed by **Morito et al** using broadcast time embedded in the watermark because it would ensure that the broadcast time information is not user set so that a user is unable to circumvent the broadcast time information. One of ordinary skill in the art would have recognized the advantages of using broadcast time embedded in the watermark as part of authentication information for authenticating the content because in the event that the time difference is not within an acceptable threshold of time the receiver would not be able to further process the content as suggested by **Morito et al** (see column 7, lines 26-35 and column 9, lines 14-20).

**As per claim 54**, the references as combined above disclose the limitation of wherein the *time identification information specifies a broadcast time at which a program including the one or more pieces of content is distributed via broadcast* (See **Morito et al**, column 7, lines 14-35 and column 9, lines 20-38). This claim is rejected on the same rationale as the rejection of claim 53 above.

**As per claim 55**, the references as combined above disclose the limitation of wherein the *time identification information specifies a broadcast time at which the one or more pieces of*

*content are distributed via broadcast* (See **Morito et al**, column 7, lines 14-35 and column 9, lines 20-38). This claim is rejected on the same rationale as the rejection of claim 53 above.

**As per claim 59**, **Levy et al** discloses the limitation of *wherein said distribution apparatus is operable to embed the authentication information into one or more pieces of the content using a digital watermarking technique*, (see column 8, lines 65-67). (For details see column 8, lines 20-30 and column 8 line 46-col. 9, line 11). (See **Morito et al**, column 7, lines 14-35 and column 9, lines 20-38). This claim is rejected on the same rationale as the rejection of claim 53 above.

**As per claim 60, Levy et al** discloses the limitation of *wherein said distribution apparatus is operable to embed the authentication information into a distribution signal of one or more pieces of the content using a digital watermarking technique*, (see column 8, lines 65-67). (For details see column 8, lines 20-30 and column 8 line 46-col. 9, line 11). (See **Morito et al,** column 7, lines 14-35 and column 9, lines 20-38). This claim is rejected on the same rationale as the rejection of claim 53 above.

**As per claim 61, Levy et al.** discloses the limitation of *wherein each content has specific content identification information, said distribution apparatus being operable to store a distribution history for each piece of one or more pieces of content distributed via the predetermined distribution path in association with its specific content identification information*, for example (see column 10, lines 19-49); *and to transfer only the distribution*

*history associated with specific content identification information by masking the distribution history for each piece of one or more pieces of content with a predetermined filter*, for example (see column 13, lines 15-22 and column 10, lines 24-67). **Levy et al** also discloses ISRC, which implicitly or inherently contains predetermined filter and unique identifier (col. 3, lines 24-28).

**As per claim 62, Levy et al.** discloses the limitation of *wherein each content has specific content identification information, said distribution apparatus being operable to store a distribution history for each content distributed via said predetermined distribution path association with its specific content identification information* (see column 10, lines 19-67*), and said monitoring apparatus being operable to cause content identification information by which said distribution history can be addressed to be contained in said authentication information*, for example (see column 2, line 61 through col. 3, line 23).

**As per claim 14, Morito et al** suggests combining a separate encrypted channel with the transmission method (see column 6, lines 5-21). **Levy et al** substantially discloses distribution of one or more pieces of the content embedded with play time captured (*time identification information)* (see column 10, lines 50-67) that meets the recitation of *distributing the one or more pieces of content together with attached time identification information in an unencrypted form* and further discloses that some identifier can be encoded and others not encoded in the content to be distributed including timestamp or time of playback (see column 3, lines 24-63 and column 13, lines 15-22). **Levy et al** discloses one or more pieces of content may be distributed with the usage rules *(authentication information)* packaged with the electronic content encrypted,

and the license server may provide software (key) for decrypting the distributed one or more pieces of content (see column 6, lines 49-60) that meets the recitation of *distributing the attached authentication information in an encrypted form encrypted using an encryption key* as interpreted by the Examiner. **Levy et al** as shown herein suggests implementing the invention using encryption/decryption by distributing one or more pieces of content with the attached authentication information in an encrypted form encrypted using a key, and discloses comparing an identifier encrypted using cryptographic algorithm to a watermarked object unencrypted form (see column 9, lines 40-67), but is silent about issuing a key and comparing the decrypted authentication information with the unencrypted authentication information. Examiner takes official notice that the authentication protocol of transmitting authentication information in an unencrypted form and the attached authentication information in an encrypted form and comparing the decrypted information in the encrypted form with the authentication information in the unencrypted form to detect the owner of the message is very well known in the art of cryptography. Therefore, it would have been obvious to one of ordinary skill in the art to modify Levy to implement this authentication protocol as mentioned above. One of ordinary skill in the art would have been motivated to do so because it would allow any device to perform authentication using only the authentication information itself that is transmitted obviating the need to compare with information from a database, thereby using fewer resources.

**Stefik** in an analogous art teaches a system for controlling use and distribution of digital work (content) containing usage right (authentication information) embodied in the digital work (see column 4, lines 35-36), the usage right includes time specification or time stamp (see column 4, lines 25-36 and column 14, lines 49-53). Transactions occurred between repositories

(monitors and distributors) (see column 26, lines 48-53) and the transactions refer to part or complete digital work (content) or digital work containing other digital works (see column 30, lines 57-62) to determine if the usage rights (authentication information) are satisfied. **Stefik** discloses one example of an authentication validation between two repositories (servers) regarding registration transaction in which encryption keys are issued (see column 27, lines 29-31), wherein the *monitoring step* includes repository-1 *decrypting the authentication information* (performance message) *in the encrypted form using the encryption key and comparing the decrypted authentication information (name of the repository and time) with the authentication information in the unencrypted form to determine whether the one or more pieces of content have been distributed with authorization of the one or more owners information* (see column 28, lines 43-59). Although **Stefik** uses public/private for additional security, a shared key could have been used as known in the art (see column 27, lines 1-10). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the distribution method of **Levy et al** to include said monitoring step further includes decrypting the authentication information in the encrypted form using the encryption key and comparing the decrypted authentication information with the authentication information in the unencrypted form to determine whether the one or more pieces of content have been distributed with authorization of the one or more owners. One skilled in the art would have been lead to make such a modification to prevent replay attack and ensure that someone is not interfering with the communication and the transaction as suggested by **Stefik** (see column 28, lines 37-41 and column 27, lines 15-32).

**As per claim 58, Morito et al** suggests combining a separate encrypted channel with the transmission method (see column 6, lines 5-21). **Levy et al** discloses a server *(monitoring apparatus)* operable to distribute of one or more pieces of the content embedded with play time captured (*time identification information)* (see column 10, lines 50-67) that meets the recitation of *distributing the one or more pieces of content together with attached time identification information in an unencrypted form* and further discloses that some identifier can be encoded and others not encoded in the content to be distributed including timestamp or time of playback (see column 3, lines 24-63 and column 13, lines 15-22). **Levy et al** discloses one or more pieces of content may be distributed with the usage rules *(authentication information)* packaged with the electronic content encrypted, and the license server may provide software (key) for decrypting the distributed one or more pieces of content (see column 6, lines 49-60) that meets the recitation of *distributing the attached authentication information in an encrypted form encrypted using an encryption key.* **Levy et al** as shown herein suggests implementing the invention using encryption/decryption by distributing one or more pieces of content with the attached authentication information in an encrypted form encrypted using a key, and discloses comparing an identifier encrypted using cryptographic algorithm to a watermarked object unencrypted form (see column 9, lines 40-67), but is silent about the monitoring apparatus issuing a key and comparing the decrypted authentication information with the unencrypted authentication information. Examiner takes official notice that the authentication protocol of transmitting authentication information in an unencrypted form and the attached authentication information in an encrypted form and comparing the decrypted information in the encrypted form with the authentication information in the unencrypted form to detect the owner of the message is very

well known. Therefore, it would have been obvious to one of ordinary skill in the art to modify Levy to implement this authentication protocol as mentioned above. One of ordinary skill in the art would have been motivated to do so because it would allow any device to perform authentication using only the authentication information itself that is transmitted obviating the need to compare with information from a database, thereby using fewer resources.

**Stefik** in an analogous art teaches a system for controlling use and distribution of digital work (content) containing usage right (authentication information) embodied in the digital work (see column 4, lines 35-36), the usage right includes time specification or time stamp (see column 4, lines 25-36 and column 14, lines 49-53). Transactions occurred between repositories (monitors and distributors) (see column 26, lines 48-53) and the transactions refer to part or complete digital work (content) or digital work containing other digital works (see column 30, lines 57-62) to determine if the usage rights (authentication information) are satisfied. **Stefik** discloses one example of an authentication validation between two repositories (servers) regarding registration transaction in which encryption keys are issued (see column 27, lines 29-31), wherein the *monitoring step* includes repository-1 *decrypting the authentication information* (performance message) *in the encrypted form using the encryption key and comparing the decrypted authentication information (name of the repository and time) with the authentication information in the unencrypted form to determine whether the one or more pieces of content have been distributed with authorization of the one or more owners information* (see column 28, lines 43-59). Although **Stefik** uses public/private for additional security, a shared key could have been used as known in the art (see column 27, lines 1-10). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the

distribution system of **Levy et al** to include said monitoring step further includes decrypting the authentication information in the encrypted form using the encryption key and comparing the decrypted authentication information with the authentication information in the unencrypted form to determine whether the one or more pieces of content have been distributed with authorization of the one or more owners. One skilled in the art would have been lead to make such a modification to prevent replay attack and ensure that someone is not interfering with the communication and the transaction as suggested by **Stefik** (see column 28, lines 37-41 and column 27, lines 15-32).

***Conclusion***

3. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. The prior art discloses monitoring and determining whether distribution of content have been distributed with authorization of the owner. (See PTO-form 892).

3.1 Any inquiry concerning this communication or earlier communications from the examiner should be directed to CARL COLIN whose telephone number is (571)272-3862. The examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser G. Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Carl Colin/
Examiner, Art Unit 2136
February 29, 2008